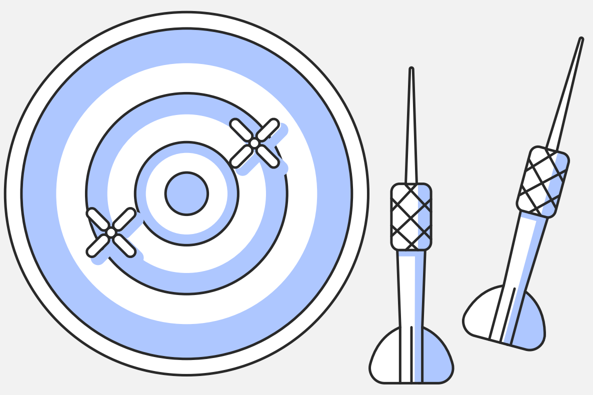
NATION STATE CYBER THREATS

Some Key Statistics 2020-2021



Cyber Capabilities Continue to Evolve

Over the last 20 years, cyber capabilities have become a formidable new instrument of national power. As well as using such capabilities to obtain state secrets from each other, as in traditional espionage, states have also used them for a range of other, more threatening purposes. These include bolstering their own economic development by stealing intellectual property; threatening to disrupt the financial institutions, oil industries, nuclear plants, power grids and communications infrastructure of states they regard as adversaries and attempting to interfere in democratic processes.

MOTIVES FOR THEIR CYBERATTACKS

ESPIONAGE

more specifically, intelligence collection, far more common goal than others

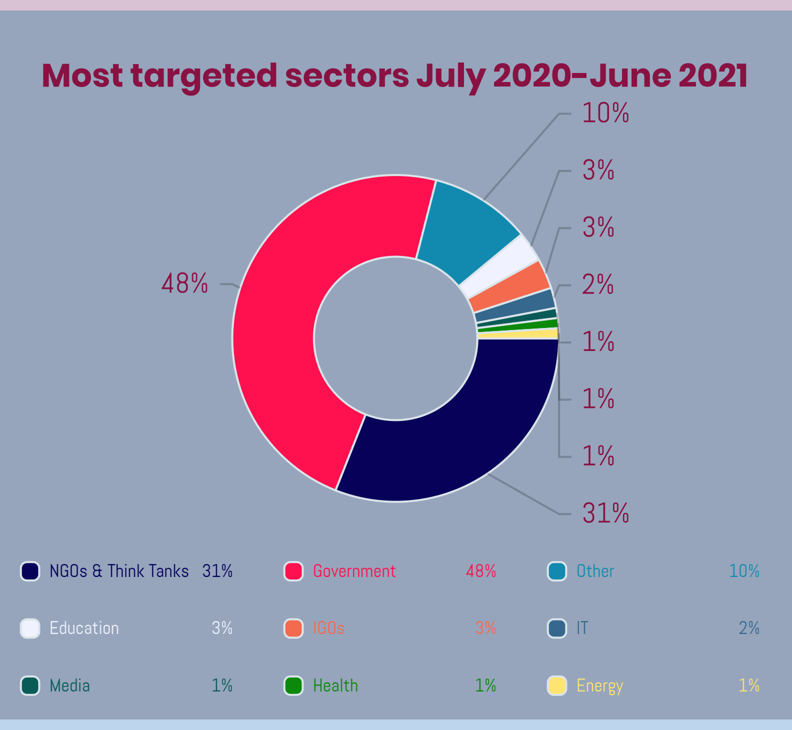
DESTRUCTIVE ATTACKS

Iran has been the only nation state actor willing to regularly engage in destructive attacks, mostly against Israel

MONETARY GAIN

North Korea targets companies in cryptocurrency trade or related research, likely seeking either to steal cryptocurrency or intellectual property

Most targeted sectors July 2020-June 2021



NGOs & Think Tanks	31%	Government	48%	Other	10%
Education	3%	IGOs	3%	IT	2%
Media	1%	Health	1%	Energy	1%

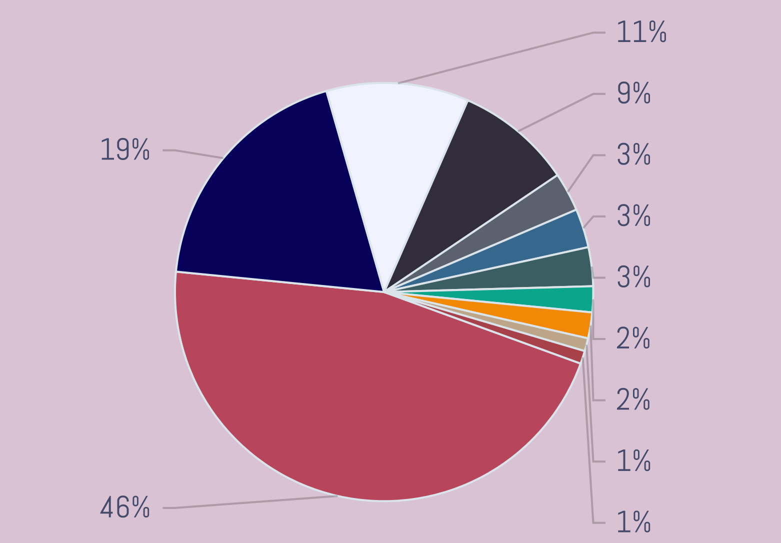
NEARLY 80%

of those targeted were either in government, NGOs or think tanks.

Government sector targeting largely focused on ministries of foreign affairs and other global government entities involved in international affairs.

Russia, China, North Korea and Iran were the most active against this sector

Most targeted countries July 2020-June 2021



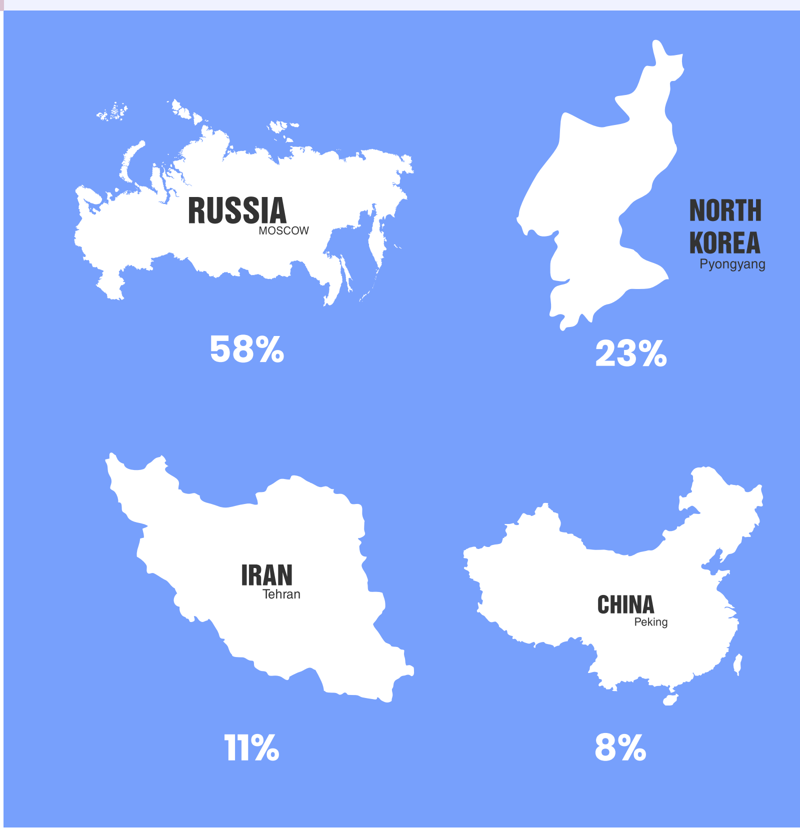
USA	46%	Ukraine	19%	Other	11%	UK	9%
Belgium	3%	Japan	3%	Germany	3%	Israel	2%
Moldova	2%	Portugal	1%	Saudi Arabia	1%		

ORGANIZATIONS IN THE USA REMAINED THE TARGET OF MOST OF THE ACTIVITY THIS YEAR

There was also an increase of targeting consistent with increasing geopolitical tensions between nations

ATTACKS BY COUNTRY OF ORIGIN

Russia's "UNC2452" and its aggressive targeting of IT service providers & Western government institutions place Russia on the top spot for countries where attacks originated this year. While North Korea's "Kimsuky" & "Velvet Cholima" come in second as a result of the strategy employed, namely relying on large quantities of attacks.



Attack vectors used by nation state malicious actors

PASSWORD SPRAY · SOCIAL ENGINEERING · PHISHING · IDENTITY SPOOFING · MALWARE · SUPPLY CHAIN INSERTION · MAN-IN-THE-MIDDLE · DENIAL OF SERVICE

Nation states are advanced enough to do reconnaissance on their victims and select the attack method that best suits each goal or intended outcome.

Source: Microsoft Digital Defense Report October 2021

Available at: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1

Security Service of Aruba

www.vda.aw

cybersecurity@vda.aw

Vigilantia Diligentia Animus